Privacy and Security Workgroup
Transcript
January 11, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, and welcome, everybody, to the privacy and security policy workgroup, which is a workgroup of the HIT Policy Committee. Just remember that this hearing is being conducted in public, and the public will have opportunity at the close of the meeting to make comment and, workgroup members, if you'd please remember to identify yourselves when speaking. Let me do a roll call now of the workgroup members. Deven McGraw?

Deven McGraw - Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Rachel Block?

Rachel Block – New York eHealth Collaborative – Executive Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Tang?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Mike Klag? Judy Faulkner or Carl Dvorak? Paul Egerman?

Paul Egerman – eScription – CEO
Yes, I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Uhrig?

Paul Uhrig – SureScripts – Chief Privacy Officer, EVP Corporate Development
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Terri Shaw? John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Joyce DuBow? John Blair? Peter Basch? Justine Handelman? Dave Wanser?

Dave Wanser – NDIIC – Executive Director
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Kathleen Connor?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anybody off?

Carl Dvorak – Epic Systems – EVP
Carl was here. I had my phone on mute when you called me.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. Thank you. I believe Sarah Wattenberg is on the line from ONC. All right. I'll turn it over to Deven McGraw and Rachel Block.
Deven McGraw - Center for Democracy & Technology – Director
Great. Thanks, Judy.

Rachel Block – New York eHealth Collaborative – Executive Director
Thank you.

Deven McGraw - Center for Democracy & Technology – Director
For those of you who do not know, the Office of the National Coordinator has established a policy whereby the workgroup meetings, in addition to the policy committee and full standards committee meetings, will be conducted open to the public. Now that doesn't mean that we could not, I there was a strong policy reason for closing a meeting, do so. But, for the most part, we are going to operate in our meetings with the public fully invited. And, as Judy explained, what that means is that they're on mute for most of the call, but we reserve the last 15 minutes of the call to open it up for public comments. Does anybody have any questions about that?

Okay. Great. Again, I think it's a welcome change personally, but it does require us to, in addition to it being easier for workgroup members to know who is speaking when they're speaking, it's all the more important for you to identify yourself when you make a comment so that all of the persons on the line know who you are.

With that, we'll move into the first item on the agenda, which is finalizing our workgroup charge. Now these are changes that I think originated with John Houston. There was one more addition of the word collection in the very end of the charge that was suggested by staff. I think a lot of folks were supportive of these changes when we circulated them by e-mail, but given that not everybody had a chance to weigh in, I wanted to spend just a little bit of time this morning making sure that everybody is comfortable with

the wording and that we can finalize it and then move on to other business. Does anybody have any questions, comments, further suggestions?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. Is it showing on the Webinar because I don't think I got it?

Deven McGraw - Center for Democracy & Technology – Director
It's on the annotated agenda. You should have received it. It's not, so I'll go ahead and read it. "Make short-term and long-term recommendations to the Health IT Policy Committee on privacy and security policies and practices that will help build public trust and help information technology and electronic health information exchange. Specifically, the workgroup will seek to address both complex privacy and security requirements through the development of proposed policies, governance models, solutions, and approaches that enhance privacy and security, while also facilitating the appropriate collection, access, use, and exchange of health information to improve health outcomes."

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Can I ask you a question?

Deven McGraw - Center for Democracy & Technology – Director
Sure.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
In that last, collection, access, use, the disclosure is not part of that list?

Deven McGraw - Center for Democracy & Technology – Director
The term exchange is used. To me, that includes disclosure.
Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I would just caution. The caution about that is that in the privacy principals and the sort of literature in terms of … the word disclosure is often used, and one could exchange health information without actually using that information. For example, when it's in transit through a clearinghouse where they may look at the header, but they're not using or really accessing the information. So that would be my….

Paul Egerman – eScription – CEO
Yes. This is Paul Egerman. I agree. There's a lot of confusion about the words access, use, and disclosure. And it seemed to me it would be easy just to throw all three of them in.

Deven McGraw - Center for Democracy & Technology – Director
Yes. This is Deven. I certainly don't have a problem with that. Does anybody object to that on the workgroup?

W
Can you just read where that would go in? I'm sorry.

Deven McGraw - Center for Democracy & Technology – Director
Sure. It would be – so it's towards the end of the charge, so it goes with our development of, again, proposed policies and models and solutions and approaches that enhance privacy and security while also facilitating the appropriate collection, access, use, disclosure, and exchange of health information to improve health outcomes.

W
That's fine.

Gayle Harrell – Florida – Former State Legislator
You have Gayle on the phone again now.

Deven McGraw - Center for Democracy & Technology – Director
Okay.

Justine Handelman –BCBS – Executive Director Legislative & Regulatory Policy
Deven, this is Justine Handelman of BlueCross BlueShield. One thought I had….

Deven McGraw - Center for Democracy & Technology – Director
Sorry, I'm echoing. I hope you're not all hearing that.

Justine Handelman –BCBS – Executive Director Legislative & Regulatory Policy
Is it also in the first sentence? Could we add in at the end of the first sentence, so it would read, you know, "Will help build public trust and health information technology and electronic health information exchange and insure its use to improve healthcare quality and efficient"? Because I think part of everything we do is not only to build the trust in it, but also to facilitate the use.

Deven McGraw - Center for Democracy & Technology – Director
Right. I certainly don't have a problem with adding that. That is exactly why the specifically line says that the solutions and approaches enhance privacy and security, while also facilitating its use.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker. Would you please read that extra?
Deven McGraw - Center for Democracy & Technology – Director
Yes, Justine. If you'll read it again, that would be great.

M
Yes, please read it again

Justine Handelman –BCBS – Executive Director Legislative & Regulatory Policy
Sure. Instead of just ending at exchange, period, in that first sentence, you'd just add on, "And insure its use to improve healthcare quality and efficiency."

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think that that's the charge of this workgroup is to insure its use.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. And, at the very least, make it authorized uses.

Peter Basch – MedStar Health – Medical Director
This is Peter Basch. I would agree. I think that exceeds the bounds of the workgroup.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If you put enable, I'd be okay about that.

W
Or facilitate.

W
Yes, and that's just the point because I think part of the whole goal in having appropriate privacy and security safeguards is to get people to feel comfortable to use it, and I just think that's important to help facilitate, but I'm fine with those word changes: facilitate, enable.

Deven McGraw - Center for Democracy & Technology – Director
Right. So in other words, it would say, and facilitate its appropriate use to improve healthcare quality and efficiency.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd leave it….

M
Why…?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Facilitate goes farther in the application domain than I think … this workgroup….

Deven McGraw - Center for Democracy & Technology – Director
Okay, so enable?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd be fine with that. This is Dixie.

Deven McGraw - Center for Democracy & Technology – Director
Okay.

John Blair – Hudson Valley HIE – President & CEO
Yes. This is John Blair. Do you have the statement up? Is it up somewhere we can look at?

Deven McGraw - Center for Democracy & Technology – Director
But if not, it was on your annotated agenda.

John Blair – Hudson Valley HIE – President & CEO
Okay, so I'll pull it up there because I remember looking at it over the weekend. But it does distinguish access, exchange, and disclosure as separate?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

John Blair – Hudson Valley HIE – President & CEO
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
…it doesn't mention disclosure right now.

Deven McGraw - Center for Democracy & Technology – Director
Yes, it does. We just approved that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well that's what I said, with the change it does.

W
For those of us who are a couple minutes late, could you restate the whole sentence…?

Deven McGraw - Center for Democracy & Technology – Director
All right. I'll do the best I can here. I also have my trusty sidekick taking some notes over here. This is Deven McGraw. "To make short-term and long-term recommendations to the Health IT Policy Committee on privacy and security policies and practices that will help build public trust and health information technology and electronic health information exchange, and enable its appropriate use to improve healthcare quality and efficiency. Specifically, the workgroup will seek to address both complex privacy and security requirements through the development of proposed policies, governance models, solutions,

and approaches that enhance privacy and security while also facilitating the appropriate collection, access, use, disclosure, and exchange of health information to improve health outcomes."

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. The word appropriate, I find somewhat ambivalent. I don't know what it means. Authorize seems to be more in line with what's allowed in a regulatory sense, and is there a reason for using appropriate?

M
I would say the reason for appropriate over authorize is that appropriate has some sense that it's those people who have a need or will have a need to access that information or use it. Authorize, I mean, anybody could be authorized, whether it's appropriate or not, I guess.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Maybe it's both.
Deven McGraw - Center for Democracy & Technology – Director
All right. This is Deven. It's a charge. It's not a statute. And the reason why I didn't devote a lot of time to doing this was because I'm not sure that it's a great use of our time to nitpick on the details of this thing.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Based upon that then – this is John Houston – I would propose then that we simply, we should get past this and get on with life then rather than….

Deven McGraw - Center for Democracy & Technology – Director
Yes. I mean, in terms of sort of – and I throw that in for the appropriate versus authorize debate. Again, for a charge, Kathleen, I get where you're going, and John, I get your counterpoint. I think appropriate sort of subsumes all of those things.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree. I move that we accept it with the changes just made. This is Dixie Baker.

Joyce DuBow – AARP Public Policy Institute – Associate Director
I support that. It's Joyce DuBow.

Gayle Harrell – Florida – Former State Legislator
I also. Gayle Harrell.

Justine Handelman –BCBS – Executive Director Legislative & Regulatory Policy
I do. Justine.

Deven McGraw - Center for Democracy & Technology – Director
Excellent. Does anybody have any strong objectives to us moving forward as I just read it?

M
No.

Deven McGraw - Center for Democracy & Technology – Director
Excellent. All right. Well I thank you all. I apologize if I was terse, but I know I heard from a lot of you after our initial call, and I know we have a large group here too, but I think it's important to have a broad range of stakeholders represented, and the more kind of focused we can be, number one, I think will advance us farther forward in making some good recommendations, and also facilitate kind of maximum participation. Again, I apologize if I was being terse, but I want us. I know we have a group here that can make some really good progress on these complicated issues, but we'll only be able to do that if we can be really focused.

Alison Gary – Altarum Institute – Communication Technologies Coordinator
Deven, this is Alison from Altarum. I'd like to remind all speakers to please turn down your speakers on your computer because that is what's causing the echo. Thank you.

Deven McGraw - Center for Democracy & Technology – Director
Thank you, Alison. That's right. Okay. All right. Terrific. Let's move then to the next item on the agenda, which is, you'll recall that one of the things that we started to talk about on our last call was this nationwide privacy and security framework for electronic exchange of individually identifiable health information. For those of you who are not as familiar with this document, this is a set of overarching principals gleaned from a number of different models of fair information practices that have been put forth both here in the U.S., as well as abroad, that was developed during the Bush Administration by the Office of the National Coordinator and released to the public in December of 2008, so really more towards the end of that year.

Folks didn't get a chance to read it really before our first call, and there have been some subsequent. There's also some concurrent work going on by a separate, strategic planning workgroup, which involves creating a white paper that expresses some kind of overarching principals in a number of key areas, and that includes privacy and security, drives down to some more specific objectives, and then moves toward a kind of strategic plan or a timeline for getting some of that work done. Again, that's a separate workgroup with some members on this workgroup also serving on that one. But, nevertheless, it's a place where they're sort of working with a set of – they want to work with a set of principals that can then get parsed into some more specific objectives and strategic plan going forward.

My hope is that we will continue to kind of work together in a back and forth way as some of these objectives, more specific objectives and timelines get nailed down because I think it's appropriate as the privacy and security workgroup that we do that. But in the meantime, what to do with this nationwide framework, I want to propose something to the workgroup now, which is to discuss whether there are any sort of key omissions in it, but otherwise not to wordsmith it. Again, it's at the more principle level, and to pass it on to the strategic planning workgroup to be incorporated as the overarching principles that would go into that white paper. I'm going to stop now and pause a second and allow Rachel to add any thoughts, and then we'll open it up for some comments.

Rachel Block – New York eHealth Collaborative – Executive Director
No, I just wanted to also hopefully to clarify for folks that as the document is structured, there is a comment to this on page five, is the first sentence after the bold heading that is the stated principle. The information in the italics, if I'm following this correctly, and Deven or Judy, correct me if I'm wrong, is really sort of the elaboration or explanation that ONC prepared to explain the principle. The principles themselves are the items, the individual sentences that immediately follow each bolded heading, so individual access, corrections, openness and transparency, choice, etc.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I think that's right, Rachel. This is Deven. Were there any, again, because essentially ONC worked on this for about two years, but since we're a new workgroup, I think it's worth noting if there are any key omissions that we would want to see incorporated in here, but to try to avoid wordsmithing it, I think that's a rabbit hole that we may not recover from for the rest of the two hours here.

Rachel Block – New York eHealth Collaborative – Executive Director
Yes. I think the other point would be that the strategic planning committee will review this is in the context of their work. They may send it back to us to day, in our discussion we think that you might want to discuss item X, which either wasn't addressed in this or might need some elaboration, so this might end up coming back to us after the strategic planning committee review it.

Paul Egerman – eScription – CEO
Yes. This is Paul Egerman. My only comment about the document, and first, the document and the framework is really excellent. It lays things out very clearly, but it was written before ARRA. And so, as a result, it doesn't refer to ARRA in any way. And I'm wondering if that's a little bit of a problem, especially

since the document says something like patients should have rights to have access to their electronic data. ARRA already gives them that access.

Deven McGraw - Center for Democracy & Technology – Director

Yes, that's exactly right, but what's interesting is that these are principals for which actually even before ARRA we had some law on. And so in some respects, one could think of this as we actually already have some law in this area that provides some guarantee in more specific ways of how these principals get operationalized. But nevertheless, to the extent that there's law in some areas, but gaps in others, when you set forth some overarching principals, it can then help guide you when you're making decisions down the road about what's the sort of overarching approach that governs what we do.

I would actually argue that because it's at the principle level that it doesn't need to be updated. Using your example, Paul, the HIPAA privacy rule has always given people the right to have a copy of their data in the form or format they request, if it was possible for the entity to give them in that format. The only thing that ARRA did was specify that if you've got an electronic record, you've got to give it to people electronically. And there's some limitation on how much you can charge them, so it's not supposed to go into that level of detail. In some respects, it's a little bit more of a living document where the policies underneath it might change, but the principals remain the same, and the policies in fact are operationalizing.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

This is John Houston. In looking through all of those, the different, what do you call them, the different policies, or I don't know. There's nothing in here that, to me, when I read through, says okay; ARRA changed that. Nothing stands out as being, you know, ARRA put this totally on its head. To me, they still are, to me, equally applicable, even now.

Rachel Block – New York eHealth Collaborative – Executive Director

Yes. I think, just to follow on, this is Rachel, on Deven's comment. ARRA provides a specific implementation context now for certain of these, and we'll be discussing that momentarily, I think, in conjunction with the proposed rules, but it doesn't fundamentally alter then.

Marianna Bledsoe – NIH – Deputy Associate Director

This is Marianna Bledsoe with the NIH. I think this is actually a very well written document, and I think these principals are really very nice. I think, as we move forward, however, in sort of implementing the principals that it'll be important to keep research uses and disclosures in mind because HIPAA currently allows some disclosures, for example for research, without authorization, the use of limited data sets, and so on. So I just raise that. I don't know that we need to change anything in the document to address that, but I think we need to keep research uses and disclosures in mind moving forward.

I also wanted to suggest a possible tweak to the charge, and unfortunately I could not weigh in. There was something. I was being blocked. My access was blocked, but that's subsequently been changed. To include research in the charge, and where I'd like to propose it is at the end of the charge where it says, "To improve health outcomes, including for research."

Deven McGraw - Center for Democracy & Technology – Director

Marianna, this is Deven. I think the only thing that gives me pause there is I'm not opposed to research, but I'm a little uncomfortable with calling one thing out that improves health outcomes versus other things that improve health outcomes. I think that we want to try to keep it brought, if we can, and if we're calling out one thing, to me it opens a door, but I want to hear from others.

Marianna Bledsoe – NIH – Deputy Associate Director

If it's understood to fall within to improve health outcomes, I'm fine with that. I just don't want it to get lost and that, as we move forward, that research uses get appropriate consideration.

Deven McGraw - Center for Democracy & Technology – Director

Okay. You're okay with not specifically mentioning it, but making sure that we shape our agenda going forward, don't leave that out, and I definitely do not want to. It's important.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen Connor. I wanted to point out that in the various statements of these principles, there's inconsistency about whether we're talking about collection use of disclosure and, in a couple of places, that's how it's stated, and then under safeguards, it's access, use disclosure, but no collection. I think it would be helpful if the group consistently used sort of the spectrum of types of accesses. I don't know what the exact term is. Particular kinds of permissions so that you had collection, access, use, and disclosure covered consistently throughout the document wherever these principles are stated. I don't see any particular reason why it's one versus the other set. For example, under individual….

Deven McGraw - Center for Democracy & Technology – Director
No, I get what you're saying, Kathleen. I think, again, to avoid wordsmithing this, how about if we, as we pass this along, note that it's not clear in every principle that the full spectrum of different types of activities with data were appropriately recognized and the strategic framework workgroup should consider that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes. I think….

Deven McGraw - Center for Democracy & Technology – Director
And we certainly will in terms of our own discussion about specific policies.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker. The key difference that I think Kathleen is pointing out really relates to data versus information because you can access data without disclosing information if the data are encrypted.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that if we were consistent in you access data, and you disclose information, we would handle the concerns that he has.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Because there are different rules that apply to them, and as Dixie is pointing out.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
The other one, and I don't want to wordsmith, but I was wondering—

Deven McGraw - Center for Democracy & Technology – Director
But—

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
But, well, I just want an explanation, actually. On page eight, under collection, use, and disclosures, it says there is the line, "Never to discriminate inappropriately," and I'm pondering, what is appropriate versus inappropriate discrimination?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
For example, Marianna's comment about research, if you do a cohort search to find a cohort for a clinical trial, you're discriminating….

Deven McGraw - Center for Democracy & Technology – Director
Yes, I'm not sure that that's what was meant. Sarah Wattenberg from ONC, do you have any idea what they were getting at there?

Sarah Wattenberg – ONCHIT – Public Health Advisor
No, I don't. I think I've heard that comment before. I can try and talk to the project officer and find out.

Deven McGraw - Center for Democracy & Technology – Director
Okay. Yes, that's a good question.

Sarah Wattenberg – ONCHIT – Public Health Advisor
Yes, and some of this stuff, this is a living document, so I'm making some notes about some of these kind of easy changes that we can think about.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, I remember that Jodi Daniel once mentioned to me that when the security and privacy workgroup of the standards committee were looking over this framework, she mentioned that they, ONC, were in the process of updating it and recognized its need to be updated. Could you get from her the specific needs for update that they already identified?

Deven McGraw - Center for Democracy & Technology – Director
Yes, I don't. The latest that Jodi had said to me was not that they were necessarily going to be updating this document per se, but that they recognized that by putting this forward that this was only the first step, and that sort of specific policies and best practices to operationalize it was going to be more the focus, but we can certainly confirm that. I did not get the sense that there was going to be necessarily further changes made to this document per se. But again, I think my view, and I sit on the strategic planning workgroup, is that to the extent that there are some key things that we want to pass along to them, and I think that's basically what we've been discussing this morning, as we say, think about this as you kind of incorporate this or discuss it in drafts of a white paper that will form the strategic plan going forward. I think that's all appropriate.

Gayle Harrell – Florida – Former State Legislator
Deven, this is Gayle. The one thing I would ask us all to look at is under safeguard when you talked about individually identifiable information should be protected with reasonable administrative, technical, and physical safeguards to insure its confidentiality. What is reasonable? I think that's where people are going to get very nervous is how you define reasonable and where that leads you, and is it going to be truly protected?

Deven McGraw - Center for Democracy & Technology – Director
I think that's right, Gayle, and it's one of the reasons why with these, sometimes language in principle form, you know, an overarching principle, reasonable, appropriate, you know, those are pretty broad terms. And the real meaning of them, I think, comes down to when you start to discuss specific policies.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and I think that we really need to be very mindful of that and what is reasonable in one person's eye is not appropriate in another.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Reasonable in the eye of the beholder.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Reasonable is in the eye of the beholder, and I think, as we determine things, we have to be very cautious that we are making things that our policies are developed to protect the information, and as "reasonable" as possible, but yet making sure that there is that integrity of the data, and that privacy and security are absolutely essential. That, to me, is the crux of the whole thing, that one word right there.

Dave Wanser – NDIIC – Executive Director
This is Dave Wanser. I agree. That same word is used pretty liberally throughout the document.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and it makes me very nervous.

Deven McGraw - Center for Democracy & Technology – Director
Well, again, keep in mind that these are just at the overarching principle stage. I'm not sure what you would replace that with, again, because there are a lot of factors that need to be considered, and when you promulgate any particular policy, and I think sometimes these buzzwords, while they make me nervous too, they're more placeholders for the harder work that we will do, quite frankly, in discussing what that means.

Dave Wanser – NDIIC – Executive Director
This is Dave Wanser. The issue for setting a principle is whether it's a minimum standard or an expectation for the highest level of performance. You could take the word reasonable out and not do any damage to the principle, but make it clear that the expectation is that these things are absolute. The policy may then need to shade the gray in it, but the overall principle should be the highest standard.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I agree with him. I'm sorry I didn't get your name. We should really – I'm looking at the principles here. In every case, you could take that reasonable word out of there and that would be the principle.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
This is Paul Tang. I wonder if maybe it would help, Deven, if I give a little bit of context about the strategic planning process. Would that be useful?

Deven McGraw - Center for Democracy & Technology – Director
Sure. Go ahead, Paul.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
So the strategic planning process, and this will be presented to the rest of the committee in a couple days. Develop four themes, and this is to remind you. This is something that's actually called from the statute that ONC update the strategic plan, and there was a workgroup formed to provide advice from the HIT Policy Committee to ONC. There were four themes that were developed to help shape the recommendations. Theme one is meaningful use of health information technology. Two is policy and technical infrastructure. Three is privacy and security, and four is create a learning health system through effective use of HIT.

You recognize that this group's efforts, privacy and security, occupy one out of the four themes. In other words, it's really major. And the way that we have organized our work is, one, to talk about the theme itself, to describe it; two, to talk about the principles; and three, the strategic objectives, and then delve into the strategy. So I think the suggestion that you've so far put forward is to use the previous framework. I don't know. There's something like six sentences as principles sound really good to me. As people have mentioned, a lot of work went into it. They described the principles very well.

Then I think what you're also talking about then is then how do you determine what's reasonable. I personally wouldn't give up the word reasonable because that reflects the balance that has to happen between where does data have to go, data information have to go in order to do all those good things: patient care, research, public health, etc. And yet, protect the individual health – the confidentiality of individually identifiable health information. And it's sometimes aggregate information. But there's always

a balancing. There's neither all one size or the other. And so I think that concept actually is at the principle level. So that may be put into context, so you can have principles, and yet the next level you'll be discussing, I think, even in this workgroup are some of the objectives that you'll pass on to the strategic planning workgroup.

Peter Basch – MedStar Health – Medical Director
Yes. This is Peter Basch. Thank you, Paul, for saying that, and I would second those comments about although the word reasonable makes some people very nervous, the word reasonable also makes me feel, as a provider, more comfortable in that the general principle is to try and achieve the balance that Paul described. I'm not opposed to listening to people's arguments about why it should come out, but I happen to be one who believes that principle of reasonableness is something that helps to protect both sides and arrive at better policy.

Deven McGraw - Center for Democracy & Technology – Director
Thank you to both of you. Again, I would propose that we send these along. I think the more important discussions we'll have about the particulars and specific policies are where we'll make our most impact and figure out how to get these policies right so that in fact we're facilitating or enabling the use of data for good benefit while, at the same time, protecting privacy. A lot of folks refer to that as a balance. Believe it or not, that's a word that doesn't always make me terribly comfortable, but I think that notion of we need to have both to do right by patients is even reflected in our charge.
Judy Faulkner – Epic Systems – Founder
Deven, this is Judy.

Deven McGraw - Center for Democracy & Technology – Director
Hello, Judy.

Judy Faulkner – Epic Systems – Founder
I've been on since the beginning, but I was – they had me on mute. I had to call back to get them to put me on speaker. Could you explain the area that says collection, use, and disclosure of limitations … identifiable health information should be collected, used, entered, disclosed only to the extent necessary to accomplish a specified purpose?

Deven McGraw - Center for Democracy & Technology – Director
Right.

Judy Faulkner – Epic Systems – Founder
And never to discriminate inappropriately. From an electronic disclosure point of view, I'm not sure what that means.

Deven McGraw - Center for Democracy & Technology – Director
Well, it's a common fair information practice concept, this notion, you know, don't collect any more data than you need to fulfill a purpose for which you are permitted, or it makes sense that you're collecting the data. You're only supposed to use what you need. Some people have come to refer to this as green use of data, kind of borrowing an environmental term. Don't collect more than you need. Don't use more than you need. Don't disclose more than you need. It also is reflected in minimum necessary standards.

Judy Faulkner – Epic Systems – Founder
Yes. Does this get into the situation where you have the patient feeling that the orthopedist shouldn't know about her depression drugs, and the orthopedist says, well, yes I should because I could kill you if I prescribe the wrong thing. Is that this sort of thing?

Deven McGraw - Center for Democracy & Technology – Director
Well, it doesn't dive down to resolve that question at that level of detail. But instead, it's a data stewardship principle that says that when you've got health information, you know, there are limits to how you can use it, so it does not specifically resolve that question, Judy.

Judy Faulkner – Epic Systems – Founder
Are we going to resolve that question?

Deven McGraw - Center for Democracy & Technology – Director
We're going to get there.

Judy Faulkner – Epic Systems – Founder
Great.

Deven McGraw - Center for Democracy & Technology – Director
Not today.

Judy Faulkner – Epic Systems – Founder
Thank you.

Deven McGraw - Center for Democracy & Technology – Director
You're welcome. Again, these are just at the principle level. All right. I'm going to propose, you know, understanding we've had some discussion about some of these, some things that I think we want to pass on to the strategic planning workgroup. I appreciate that folks were good about not wordsmithing this too much, but I'm going to propose that we, with the couple of issues that we raised being communicated also to the strategic planning workgroup, to go ahead and move this over to them for consideration as the sort of overarching principles that will guide further work in the strategic plan on privacy and security, again just at the principle level, understanding that it doesn't resolve all the details, and it shouldn't. But just at a principles level. Do folks have objections to that?

Gayle Harrell – Florida – Former State Legislator
I would just note that I would like a further discussion of that term reasonable….

Deven McGraw - Center for Democracy & Technology – Director
Right. I think I'd like to propose that we pass that along with a full understanding that while for some people that's the comfort level that the balance will be appropriately struck, for others it makes folks uncomfortable, and that what's reasonable at any given circumstance is in fact what needs to be sort of determined by more specific policies.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
And also you have at your disposal creating objectives, so if the principle is reasonable, and yet that is undefined or not precisely characterized, then one of the objectives that either ONC or the policy committee is to delve into that and say how do we hear the balance of objectives and then create a policy that reconciles all the needs. Clearly, NCVHS, for example, John Houston, is a cochair of that privacy and security committee at NCVHS, has done a lot of work on it, so there are a number, and Deven's group. There are a number of folks that have already commented on that, and maybe one of the objectives is to look at all those things as part of its preparation for new policy. Do you see what I'm saying, Gayle?

Gayle Harrell – Florida – Former State Legislator
Yes.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
So we have a principal, and then objectives can help sort out, for example, the term reasonableness.

Deven McGraw - Center for Democracy & Technology – Director
Right. I think, to the extent that there's a fair amount of over – you know, that we've got a strategic planning workgroup, and yet to the extent that objectives may be discussed on privacy and security, I know that I'm going to want to bring those to you all for further discussion, that in fact what we're doing should inform what they're doing. So you have Paul Tang and I, and I think there are others who serve on both. This privacy and security group should have, in my view, should have an opportunity to shape what goes in that work plan.

Gayle Harrell – Florida – Former State Legislator
Absolutely.

Deven McGraw - Center for Democracy & Technology – Director
Terrific discussion, folks. Thank you very much. Moving on to the next item on the agenda, let me take a step back a minute and set a framework here. One of the things that we discussed in our last call was a tentative work plan for moving our work going forward. Rachel and I are still tinkering with that a bit, but I actually think it's – and then in the interim, what happened was the release of the meaningful use proposed rule by the Center for Medicare and Medicaid Services, and the release of the interim final rule on certification criteria, both of which had sections on privacy and security that I think are definitely worth discussing, and actually raise issues that we had tentatively teed up to be on our work plan for the first quarter of our time together. And that includes sort of how to operationalize some of the new accounting for disclosure provisions that were in ARRA, and also security practices and policies.

I thought it would make sense, given that these rules do have a comment period of 60 days, which is rather generous, but we actually have a slightly shorter time period if we wanted to tee up to the policy committee some recommendations that we would seek their endorsement on before forwarding them to CMS and ONC, which makes them, in my view, a more powerful set of comments on what was put forth in both of these rules. With that, what we sent you in the agenda was links to what's called the prepublication version, and what that means is that it's the version before it's officially put in the federal register, but it's still available from a public source, and I notice that the links weren't working too well for me over the weekend, so I resent you all the hard copy documents because I took the liberty of kind of highlight for you, because they're really big rules, some of those areas where the privacy and security provisions are discussed in some more detail.

Now these page numbers won't work for you anymore once the official rule appears in the federal register because the page numbering is a little bit different, but nevertheless, it should do for us for at least a few days, and I'll try to ask my policy council if she'll find the page numbers in the new rules when they're published. So the bottom line is that if we're going to seek to put before the policy committee some recommended, some specific concerns that we want to have addressed in these rules before they are "finalized", we really ought to do that, and be ready to do that before the February policy committee meeting, and we do have at least one more and maybe even two more calls scheduled before that, so there is time in which to get that done, but I wanted to at least begin discussing and start sort of collecting issues and concerns on this call today with the hope of maybe putting before you some maybe straw man, straw dog, as my friend Micky Tripathi likes to say, proposals that we can talk about at our next call.

Specifically on meaningful use, what you've got there, and I'm really focusing on what eligible professionals, which is the individual provider side, and what hospitals have to demonstrate in order to be eligible for federal funding under ARRA. And the measure is really, there are objectives, but the measure is really, in my view, where the rubber hits the road, what they're actually going to have to demonstrate. And that is that they have to conduct or review a security risk analysis per the security rule, and then implement security updates as necessary. I presume that this is reported through attestation, which is how most of the meaningful use measures are reported to CMS. And then the certification criteria, which, on a broad level, are those criteria that have the technical functionalities that have to be in the electronic health record technology in order to support achievement of the meaningful use objectives.

There, to me, the focus seemed to be more on some security measures, including encryption and decryption, audit log requirement, mechanisms for verifying that the information hasn't been altered in transit, cross-enterprise authentication, and then an ability to record certain information on disclosures for treatment, payment, and operations, and this is related to the changes in the accounting of disclosures requirements that were part of the stimulus legislation. For those of you who don't know, currently people have an ability to get an accounting of disclosures from their medical record, but any disclosures for treatment, payment, or healthcare operations, as defined in HIPAA, did not have to be included. In ARRA, Congress took that exemption away and said to ONC, you've got to develop a technical standard

to facilitate the reporting of these disclosures. And then, consequently, the Office of Civil Rights needs to come up with a regulation that specifies in more detail how that'll get operationalized.

I'm going to stop there and just open this up for comment. We've got some note takers here. Again, we want to just try to have a rich discussion about issues, concerns. Is it sufficient? Is it not sufficient? Is there enough of a connection? What's missing? Are we happy? Again, we'll take notes on this and try to come up with and structure a discussion that might lead to recommendations on our next call. Rachel, I've been talking for a while today. Is there anything I missed?

Rachel Block – New York eHealth Collaborative – Executive Director
No, I think you've got it.

John Blair – Hudson Valley HIE – President & CEO
Deven, Rachel, this is John Blair. Is it too simplistic to say in the first piece at least initially it's an attestation thing for the providers, and in the second it's a systems capability, a technical systems capability?

Deven McGraw - Center for Democracy & Technology – Director
I think that's exactly right, John.

John Blair – Hudson Valley HIE – President & CEO
Yes.

Deven McGraw - Center for Democracy & Technology – Director
In fact, they're pretty clear in the certification criteria that this is not – that there are two separate rules. That the certification criteria interim final rule is really only about the functionality that has to be in the system, not about – so arguably, it's not about whether you use it at all.

John Blair – Hudson Valley HIE – President & CEO
Yes. So in that document that came out last week and the second piece on the systems capability, my read is if you have a certified system, that will take care of that. Now they point out that by having a certified system doesn't take care of your HIPAA requirements, but it takes care of this piece on the security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Could I point this out? This comes out time and time and time again in our work on the standards committee. The ARRA requires two things in order to get reimbursement. One is that an eligible professional or eligible hospital has to acquire certified technology, and that's what the standards document specifies the requirements for getting that technology certified, so a vendor would be most interested in those standards. Then the second thing that's required is that they demonstrate that they're using that technology meaningfully, and that's what the meaningful use measure should apply to, so that's what the individual organization should pay attention to. So standards are for vendors or people who are developing systems, and meaningful use criteria are for users.

But the point that I've often pointed out is that there are – just because a technical capability is in the technology doesn't mean that it must be used or how it must be used or anything like that. So I think, for this group, we really should be paying attention to kind of the intersection of the technology, given that they've acquired a certified system, what do they need to do to that certified system with that certified system to use it meaningfully.

M
Practically speaking, how are you going to test for that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We won't. Deven was just saying, it's by attestation.

Paul Egerman – eScription – CEO
This is Paul Egerman. I'd say thank you, Dixie. The summary you gave about certification was very good. I'm actually one of the cochairs of the certification workgroup, and so the concept for certification is that these are simply technical capabilities, and so the issue about how you tell whether or not somebody is using them is a very good question, but it's really like two different questions in front of us. One is what should be in the second on meaningful use on privacy and security. In other words, what is written here is, is that adequate? And there's a completely separate question, which is, is the certification for privacy and security, is that criteria adequate? These are two very different things.

The certification workgroup basically said the certification criteria for privacy and security should be robust. It should allow any purchaser of these systems to be able to fully comply with the law: the law being HIPAA, the law being any other law, regulations that might apply to privacy and security. And by saying it should allow the user to do that is, of course, exactly as Dixie said. That doesn't necessarily mean … and the materials … that the user will do it. This is just a technical capability.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
It's Paul Tang. On the user side, which is the meaningful use side, the criteria that CMS proposed was that the organization do a security risk assessment and act upon that. So that's the "test" on the user side. So I think it would be very interesting from the policy committee to have this workgroup feedback or comment on that NPRM for the privacy and security section because, as Deven pointed out, we're going to provide something back to CMS indirectly. It goes through ONC because we're an advisory to ONC. The comment on the rule and so you have two sort of opportunities to advise future recommendations forward. One is to the comments on the NPRM or the IFR, and the other is to objectives, strategic objectives for ONC through our strategic planning workgroup.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Can I tell you what bothers me, and this is just a context thing? Theoretically, I believe, and this is Dixie Baker once again. Theoretically what they say in the meaningful use should be adequate. You do a risk assessment. You identify what your vulnerabilities and risks are. And then you use the technical capabilities that are in your technology to counter those risks.

What we know from the security hearing that we had for the standards committee is that 48% of the people who responded in the HIMSS 2009 survey, which were mostly large hospitals, 48% do not do an annual risk assessment. Up until that testimony, I for one thought that most people were already doing a risk assessment. And I would look at this, and I would say, well that sounds pretty reasonable. But the fact is, they're not even doing the risk assessment to begin with, which makes me question their capability or motivation to really even do this measure that's in the meaningful use.

Paul Egerman – eScription – CEO
This is Paul Egerman. That's a good comment, Dixie. One question that I have, as I think about this, is do people know what a risk assessment is? I mean, should there be a greater definition of what a risk assessment is?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston. I agree with Dixie Baker. I think there's a wide variation as to compliance with things like HIPAA and ARRA and institutional maturity around this whole idea of risk assessments and compliance, for that matter, frankly. I think it would shock people to know how noncompliant some institutions really are.

M
Isn't this an opportunity to affect that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Gayle Harrell – Florida – Former State Legislator
And what verification do we have that once they do a risk assessment, if they know what it is, what measures have been put in place to rectify that? Do we have a way, other than attestation, to know that measures have been put in place to rectify things?

Rachel Block – New York eHealth Collaborative – Executive Director
This is Rachel. I think that's a very fair comment if you take this out of context, but I would point out that the entire stage one, and please correct me, Deven or Paul Tang or somebody else is if I'm wrong, is based on attestation.

Peter Basch – MedStar Health – Medical Director
This is Peter Basch. That's actually correct, Rachel. I'm sorry. I was talking, and I was on mute, and couldn't understand why my voice wasn't coming through. Sorry. I should have that problem more often.

Deven McGraw - Center for Democracy & Technology – Director
Technical capability.

Peter Basch – MedStar Health – Medical Director
Right. I couldn't see the button. But anyway, I think you're absolutely correct that once one goes past 2011 or stage one meaningful use, we would have every right to expect other information about perhaps what vulnerabilities were exposed in a security assessment and what remediation tasks were taken. Right now all you have to do is attest that you've done it, but as Rachel said, that's the schema for initial meaningful use because we want to make it something that is doable by most willing providers and implementable by TMS. But certainly going into stage two, my hope is this workgroup will come up with, just as other workgroups are coming up with more robust measures for stage two and three, that we come up with something that makes sense to actually show that people are not just clicking a box, signing a form, and not even knowing what they're doing.

W
Right.

John Blair – Hudson Valley HIE – President & CEO
But are we assuming blind, unaudited attestation?

Peter Basch – MedStar Health – Medical Director
No. Gosh, no.

John Blair – Hudson Valley HIE – President & CEO
So the attestation becomes real.

Peter Basch – MedStar Health – Medical Director
Of course it is.

John Blair – Hudson Valley HIE – President & CEO
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes, it's under penalties if you're caught.

John Blair – Hudson Valley HIE – President & CEO
Yes, so that change, I mean, that would change right there your 48%.

Peter Basch – MedStar Health – Medical Director
Well, I think the distinction – that's John?

John Blair – Hudson Valley HIE – President & CEO
Yes.

Peter Basch – MedStar Health – Medical Director
Yes. I think the distinction is there may be – I'll speak to providers because I'm more comfortable with making a blanket statement like that since I am one that a provider might click an attestation that they did something with an allergy list, and most providers know what that means. I would think hospitals know what a security assessment is. I would think that most providers would need help understanding what a security assessment is, so they may click it thinking that they've done one by perhaps checking that their server is locked in a room, and say, well, I guess that's a security assessment. I think that, yes, attestations are taken seriously, but it is true there may be a certain level of providers who don't fully understand what doing a security assessment means.

John Blair – Hudson Valley HIE – President & CEO
Yes, and that's my big concern. I'm not as worried about—

Peter Basch – MedStar Health – Medical Director
Fraudulent attestation.

John Blair – Hudson Valley HIE – President & CEO
Yes. I'm not as worried about that if they truly do audit this, and I'm not as worried about the larger institutions doing this that didn't do it before where you had that 48%. My concern is, as you point out, Peter, that we took the small practices, that they really even understand what this is. To me, that's the biggest lift.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
This is Paul Tang. Maybe I can add a format for how you can package up your recommendations feeding forward. The three opportunities: one is to comment on the NPRM. What CMS through ONC would really appreciate is if you have a comment on the proposed rule, what is your alternative, and what's the rationale behind your comment, and what is your proposed alternative and its rationale? If we're saying attestation is not good enough, well, what is the alternative? What's the rationale?

There's an opportunity that was mentioned, which is, in 2011, it may be this proposal, but in 2013 and 2015, it may look different. So we, the policy committee, are also looking for your guidance on what would you propose for 2013 and 2015?

And the final thing was the strategic objective for ONC, updating the strategic plan. So what was most recently mentioned is, well, we need to educate, particularly the smaller practices without the larger number of FTEs or support, what does it mean to conduct a security risk assessment. And is that something that the regional extension centers could help with? These are examples of concrete ways that this group could forward a recommendation onto the policy committee.

John Blair – Hudson Valley HIE – President & CEO
Could I also suggestion one other thing, Paul? This is John. There's an interesting dilemma here as well because, under ARRA, there is going to be increased audits that are going to occur, and I think it would be the question of what will happen if somebody attests to having adequate security in place and gone through all this process and done all these risk assessments and the like, and then somebody come in and do an audit and find out that they didn't comply, and then this organization having already received additional funds through this, you know, through the meaningful use. I guess the question is how is the

payment of those funds going to get – are they going to be asked to give back funds? Are they going to be told that they didn't in fact certify meaningful use? You know where I'm going with this/

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Yes. Actually, one of Deven's brain childs is the proposal she made to the meaningful use workgroup about how to "enforce" this in a way. So she came up with the proposal that your meaningful use incentives would be held back if you were found not to be in compliance with, for example, the HIPAA security rule. That was taken out in this NPRM. It would be interesting to know from this group, as the group that's delving into this particular category, what your thoughts are, what your comments are about that change.

Peter Basch – MedStar Health – Medical Director
This is Peter. I think it's two separate questions though, unless I'm misinterpreting what you said, Paul. One is that the current proposal, even by attestation, is for all or none. So providers and hospitals have to attest that they're compliant with every attestation under the ARRA to get the money. And if they're not compliant with the securities risk and privacy, then the meaningful use incentive is withheld. I thought what the other person on the phone – I'm sorry I forgot your name – was asking was what happens retrospectively if an audit is done, and you attested to everything, so you got your payment. And they found that, by audit, you actually hadn't done something, which can be separated into was it a willful false attestation? You said yes, and you didn't do it. Or you attested to it, but it was not adequate. I think those, again, are parts A and B.
My interpretation, based on how Medicare or, rather, CMS deals with other payments that are found out later by audit to be inappropriate is they ask for their money back, sometimes with penalty. And that would be my expectation for a false attestation, determined to be false, retrospectively by audit. I would hope that wouldn't necessarily be the case by an attestation that was done in good faith that somehow was done because of ignorance. However, based on how CMS deals with other payments, ignorance of a requirement is not an excuse for not having done it correctly.

Deven McGraw - Center for Democracy & Technology – Director
Right. I think the other thing to keep in mind is that meaningful use and whether you're attestations for any of the criteria are accurate and not false, that would be up to CMS to determine because they oversee the meaningful use program and those payments. However, the increased responsibility on the Office of Civil Rights to audit is with respect to the HIPAA privacy and security rule. On the one hand, if an OCR audit uncovers a security rule violation, unless there's a connection to the meaningful use payment, which doesn't exist today, there wouldn't be any impact. And so what Paul was explaining was something that I had suggested that if you're an entity that's under formal investigation for a HIPAA violation, you ought not to be getting payments, even though those are coming from CMS, under this sort of theory that it's all out of the Federal Treasury in one bucket or another, until that gets resolved.

Paul Egerman – eScription – CEO
This is Paul Egerman. This is—

Deven McGraw - Center for Democracy & Technology – Director
Quite frankly, what's on the table.

Deven McGraw - Center for Democracy & Technology – Director
Yes. This is Paul Egerman. This is an interesting discussion, but it seems to me that the topic on the agenda, the number one issue that we need to discuss is what is written here, and this meaningful use NPRM with attestation about a security audit. Is that adequate? In other words, do we have any comments about that? That's our number one issue. These other issues are important and interesting issues, but that's the number one issue that we've got right here is do we think what's written here is reasonable? Do we want to make any comments about it?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. On that note, I was wanting to know if Dixie thought that having providers purchase certified EHR technology that meet the security standards stated in the interim final rule would, to a

certain extent, give them a leg up on what they should be looking at from a risk assessment point of view and possibly move them a little closer to being able to do a reasonable job on that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, obviously it will provide them more technical, I mean, every one of these products will have security capabilities like authentication capability and access control and auditing, etc., as required by HIPAA. But it comes back to – I think it was Paul Egerman maybe that confirmed, and the HIMSS survey that we heard reported, that people aren't doing the risk assessment to begin with. It's not that they lack – I suspect most of them today have the capability to, the technical capabilities to implement security functionality that's needed, but they aren't doing it. I think that that's the big issue, and I think that we might be able to do … but if we could reach out and identify those things in particular, additional risks that having an EHR introduce into an enterprise that they didn't have before.

Deven McGraw - Center for Democracy & Technology – Director
Right. Dixie, this is Deven. Can I ask you a couple more questions on the existing security rule requirement to get a risk assessment done? Is that conducted internally, or do you have to hire outside entity to do that assessment? Is the rule at all specific on that, and is there any guidance about what an appropriate risk assessment would look like that might be out there, but providers just may not be aware of it?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The rule itself does not say that it has to be an external. It's just an internal risk assessment. It just says that you're supposed to do it annually. You can go up and Google security risk assessment, and there are plenty of guidance out there. We've been doing security risk assessments forever. But they just aren't doing it.

Deven McGraw - Center for Democracy & Technology – Director
That's right, but getting to the question that I think people raised earlier, which I think is something that I want to try to get a little bit more information on and try to shape into a recommendation is, again, guidance for these providers and mainly the small ones who they're not doing it in part because they have no clue….

Judy Faulkner – Epic Systems – Founder
Deven, this is Judy. Deven?

Deven McGraw - Center for Democracy & Technology – Director
Yes, Judy. Go ahead.

Judy Faulkner – Epic Systems – Founder
I'm wondering, and I don't know whether this helps you because you might have to do things in a certain order, but I'm wondering if we're putting the cart before the horse. To some extent, testing for security and privacy depends on what we decide we have to do electronically, and so it could be anything from it's opt in or opt out. Okay. We can check that. To a whole complex list of things, which might take several thousand hours. And until we know what it is we're testing for, it's a little hard for us to say that because then, of course, your enterprises, large enterprises can deal with a thousand hours or several thousand hours, but the small ones, of course, would struggle.

Deven McGraw - Center for Democracy & Technology – Director
We wouldn't ask people to do risk assessments for policies that have yet to be developed, and we're not without law. What they're being asked to do is a security risk analysis per existing law. They don't need to speculate about what we might decide in the future. Of course, if there are further policy developments, ideally per our recommendation, that get promulgated, then that changes the dynamic.

Judy Faulkner – Epic Systems – Founder
That's what I'm saying. Yes, that we have to keep that in mind.

Deven McGraw - Center for Democracy & Technology – Director
Yes, just existing law.

Judy Faulkner – Epic Systems – Founder
These two things work together. The complexity of what we do later on will affect the testing.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Deven, this is Paul Tang. In response to your question about the security rule itself, in the preamble to the rule, they did explain how, depending on the complexity, as you pointed out, it can be a big thing or, in smaller settings, something that, you know, it can be either done by your own staff or external parties.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Then what wasn't available when HIPAA security came out are these rec centers, for example. Perhaps since they target the smaller practices, maybe they do come up. One of their central national tests is to come up with some guidance about security audits, and that could be very useful for small practices, and they can even label it as what's the target market for their use.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. I'd like to comment on that as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we tend to blame this on small practices, and it's not.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
I understand.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That number of 48% that do not do are all large hospitals.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Dixie, I wasn't commenting on what people do or choose not to do. It was more the resources to even have a security audit plan in place. Those, I think the smaller practices don't have uniformly. It's a separate issue whether people who have the resources do an audit and don't do that. That's another dimension.

M
But in the small practices, it's probably 95+%.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Right.

Deven McGraw - Center for Democracy & Technology – Director
That figure is probably higher. I heard Gayle trying to pipe in here.

Gayle Harrell – Florida – Former State Legislator
Yes, I'm trying to get in there. I also would like to comment on the small practices that of course RACs are limited to primary care. There are a lot of small practices out there that we also want to be part, and we want everyone to have an EHR, so you've got to really make sure that there's a way to educate all practices, not just the primary care practice.

M
I think the RAC was just an example of mechanisms to do this. I mean, I really believe it's going to have to be part of routine implementation across the board.

M
Right, but what the RAC can do for primary care practices, it can create perhaps a workbook or a handout that can be utilized by other practices.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Exactly.

M
Yes. I mean, all of these.

Gayle Harrell – Florida – Former State Legislator
I would wager that 95% to 98% of practices under 50 doctors do not do a risk assessment on this.

M
Of course not, but they certainly would if they knew what to do, and if I could invoke the word reasonableness again. If what they had to do was something that was relatively simple that they could do, or designate their office manager to do, then they would certainly welcome it as part of the routine annual workflow.

M
Yes, and that was one of the points on Paul's comments on the three pieces: the attestation 2013 and then education and training.

Deven McGraw - Center for Democracy & Technology – Director
Right. Thankfully there is a vehicle for that, and I think those are important. It's not a perfect vehicle, given that it doesn't cover everyone, but it's a better start than we might have if we didn't have that resource available. What about though, connection to the certification criteria? Someone started to raise this point earlier in our conversation.

We've got this new, technical functionality, you know, these technical functionalities that the electronic health record technology now has to have in order to be certified. But it's not, you know, those aren't connected in any meaningful way, forgive the pun, to the meaningful use security risk assessment, at least not in an obvious way. And second, the other thing that sort of struck me in looking at these standards is that they were all good, from what I could tell in my limited experience with technical functionality, but no requirement to use any of this.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But that is a meaningful use requirement. You know, there should not be in the….

Deven McGraw - Center for Democracy & Technology – Director
I'm not suggesting, Dixie, that you put the requirement in the certification piece. What I'd like to discuss is whether there is some room for some requirements to use these technical functionalities, either as part of meaningful use, or as something we would recommend to OCR with respect to updating either the regulations or guidance under the security rule.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. I would strongly concur with you, Deven, on that, that there should be more specific measures of using those security standards, and I would just note in passing that access control did not appear on that list, which seems to be a huge gap.

M
But can't you tie that in with how you clarify the risk assessment?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That was their intent. I think the question is whether we want to add – and I think it's a valid one – whether we want to recommend additional specificity to the meaningful use thing of implement security updates as necessary, like do we want to provide them some specifics like, for example, here's a good example, I think. The criteria standards require that they be able to encrypt. Do we want to say in the meaningful use side of things that if you store PHI on a mobile device like a laptop or a USB drive or cell phone or whatever that the data must be encrypted, versus data that's on a server in a data center that really is not subject to as much risk of disclosure, inadvertent disclosure that's something on a mobile device that you're carrying around?

Paul Egerman – eScription – CEO
Yes. This is Paul Egerman. I think your comment there, Dixie, is really a very good comment. I want also to take a minute and get back to two issues that Deven raised. One was the disconnect between the certification criteria and the meaningful use measure, and the second one was related to what you're saying, Dixie, about sort of requirements to use this stuff.

On the first one, on the disconnect, actually, I don't see that as a problem. I think that … IFR for certification and for privacy and security really should be more robust than what you have in meaningful use because you can't test for everything, and you're not going to require meaningful use measures on absolutely everything, so I think it's really okay that there's some level of disconnect there.

The issue of the required use, which is what I think you're referring to, Dixie, is an interesting issue because one of the things that I didn't understand what this Table 2B and the whole long description about encryption that came first. It almost seemed to say, well, this is what we would like you to do, but you don't have to do it. And I kind of would like to turn that around and say, well, these are the minimum requirements. You have to do this or something better within the certification process. And I think that that would be good. I don't think you necessarily have to connect everything you do in the certification process back to some meaningful use test. The meaningful use test can just test a few of these things.

M
So if you call that out in the risk assessment, and you have those minimum thresholds, doesn't that do that?

Deven McGraw - Center for Democracy & Technology – Director
Well, I think that's an interesting question. It's not entirely clear to me what implementing "security updates" means. Does that mean having the functionalities present in the technology you're using, or does it extend to actually using it? It feels like the dots are not fully connected.

M
Yes. It's too amorphus, but if you do call that out and clarify it, does that get at what you need?

Deven McGraw - Center for Democracy & Technology – Director
I think that's part of it, but I think I'm also asking a little bit of a bigger question, and it goes to Dixie's point, although I'm thinking about it not in quite the specifics that she raised. That is, I think that there's only so far you can go with meaningful use in the criteria that you're setting because docs and hospitals and other eligible providers have to meet every single criteria in order to be paid their meaningful use payment. And so if you load too much up into that bucket, and this goes to what Paul Egerman just said, we're going to be in trouble vis-à-vis adoption.

But that's not necessarily the only policy vehicle we have for strengthening security. We also could make recommendations about the security rule. Now that's not within the policy committee's purview per se, but I'd still like to see us do that only because I think it makes an important statement about how merely

having the technical functionality in a system that doesn't get you to a more secure data environment in this space.

M
But if you had the technical capability and the attestation through the risk assessment that calls out certain things specifically as minimum requirements, that starts to get you there. And then the 2013, you can even move to testing.

Gayle Harrell – Florida – Former State Legislator
This is Gayle again. Security and privacy are absolutely the foundation of getting the public to buy into the whole concept. And I think, if you want to call things out, and want to really put meaningful use requirements in, this is the one area that you need to do it very specifically. And I would go and say, we need to have a stronger meaningful use component in security and privacy than anywhere else. And yes, it does put a burden on providers, and does put a burden on hospitals, but this is the one area where I think it is very valid to do that, even beyond attestation.

Paul Egerman – eScription – CEO
Yes. This is Paul Egerman. Those are good comments, Gayle. My observation, though, is that you can do some of this actually on the certification side. If, for example, you say that all electronic health records have to be certified that they encrypt all the data that is stored at rest, well, it's very hard for a small group to buy a certified medical record and run around that. There's no reason to undo that capability if you really wrote it right into the certification criteria, so that's a place where you could put in the specificity I think that you're looking for, Gayle.

The part that gets very hard when you do these things is privacy is really not a technical issue. It's really all about policies. We can do everything you want about sign on security and encryption and all kinds of fancy buzzwords, but if people don't have the right policies in place, if they put their passwords on their computer so everybody can see what the password is, there's not much we can do about it. It's not a technical issue. It's not even a meaningful use issue, I don't think.

M
But they've never had attestation audit and remediation before.

M
…audit before.

Gayle Harrell – Florida – Former State Legislator
There has been audit before.

M
For this?

Gayle Harrell – Florida – Former State Legislator
Medicare audits all the time.

Deven McGraw - Center for Democracy & Technology – Director
No, a different audit, like an audit log requirement, Gayle.

Gayle Harrell – Florida – Former State Legislator

M
I see what you're saying.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. Deven, your comment about recommending changes to the security rule itself, if that were truly an option for us, I think that that's the way you would want to go. And I think, what you would want

to do, and actually, our committee actually talked about this or our workgroup on the standards committee is you know, we all know that in the security rule there are a number of required standards. They call them standards. Required provisions, and there are even more addressable implementation specifications, which addressable means that they get an option as to whether to implement them or not. That was written in, what, late 1990's, right? As organizations are implementing EHRs, is this a good time to go back to those addressable provisions and perhaps make some of them required?

Deven McGraw - Center for Democracy & Technology – Director
That's essentially what I was hinting at. Now, again, so we're not – the policy committee that we report to is not an official advisory body of the Office of Civil Rights, which now has oversight over both the HIPAA privacy and security rule. But having said that, for example, we reached out to Sue McAndrew, who is the deputy director of the Office of Civil Rights, just to see if she was interested in hearing from us on recommendations for implementation of the accounting of disclosures requirement. And she said sure, yes. You know, we have limited ability to cry fowl if any recommendations we would send up on the security rule per se weren't adopted because we're not really an official recommendation body for them, but that that doorway has been opened, and I think we'd be really confined in what we could do as a workgroup if some recommendations with respect to the basic set of rules that govern this data at a federal level was off the table.

Paul Egerman – eScription – CEO
This is Paul Egerman. Those are good comments, Deven. The question I have though is, as I look at the agenda, we're supposed to be deciding if we, as a workgroup, want to make a comment about this NPRM. Is what we're really saying that what's … NPRM is okay. But we're not that excited about it because there are a lot of other issues, and so we need to go further. But we think what's written in the NPRM is okay.

Deven McGraw - Center for Democracy & Technology – Director
No. I think folks had some suggestions of things that we would do to sort of beef up, you know, more on the education side and then maybe making some more specific comments with respect to stage two of meaningful use, which we assume is about 2013 to 2015.

Paul Egerman – eScription – CEO
Yes.

Deven McGraw - Center for Democracy & Technology – Director
So I don't think we necessarily are silent on that, but you're right, Paul, in the sense that if we're going to go to looking at making recommendations for the security rule, we're not confined by the timeframes of comment on the rule that exists.

Paul Egerman – eScription – CEO
Yes. My question is, for stage one, for what's written in this NPRM, which is really you've got to attest whether or not you've done the security audit. Are we happy with that? Do we want to recommend any changes to what's written right there?

Dave Wanser – NDIIC – Executive Director
This is Dave Wanser. I think we've talked about security pretty thoroughly. What we've not talked about is privacy, and I think the second care goal is something that also requires a measure.

M
But back to the earlier comment though. How do you measure privacy? That's … security….

Dave Wanser – NDIIC – Executive Director
There are issues around transparency of data sharing that could be attested to.

M
The but to it is that, I mean, again, it's easy when you're dealing with bits and bytes and things that you can check off as saying yes or no to … scale it to hundreds of thousands of providers. I'm just worried that it's not reasonably measurable.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. Aren't there some federal laws that many providers are supposed to be able to support for privacy that we could test? For example, whether a provider can support a 42-CFR consent directive.

Deven McGraw - Center for Democracy & Technology – Director
Are you talking about under part two? But that's a limited set of providers that are subject to part two.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Right. Are there other ones that we could use…?

M
You could point to HIPAA. You could put the ARRA privacy rules, but that's the whole question of audit comes in, and the idea that the … what happens if somebody says they attest to it, and then CMS comes in and audits them and says, no, you didn't comply?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Another example that I'm thinking of is, in HIPAA, you have to be able to support authorization to disclose to, for example, the Social Security Administration, I believe. Is that correct, Deven?

Deven McGraw - Center for Democracy & Technology – Director
There are a whole set of authorizations that are required under, you know, certain data uses require an authorization. Certainly, under certain state laws require, you know, that already require consent to disclosure certain types of information. If we didn't do another thing on that issue, there's still already law.
M
Yes, but the question, I mean, outside of a complaint, how is that being checked?

Deven McGraw - Center for Democracy & Technology – Director
Right. That's the only way it's being checked.

M
Right. Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, the comment, I don't know who it was, but about transparency.

Deven McGraw - Center for Democracy & Technology – Director
That was Dave, right, Dave Wanser?

Dave Wanser – NDIIC – Executive Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Does the outcome priority of engaging patients, is that what he was referring to? Does that come within our purview?

Deven McGraw - Center for Democracy & Technology – Director
It doesn't per se, but what was your comment, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I was just wondering because they've got some specific measures there, you know, some percentages, and I thought that that's what he was addressing.

Deven McGraw - Center for Democracy & Technology – Director
I think this is different, Dixie. This is, so if you look at the particular set of care goals in the privacy, in the meaningful use rule, and this came from the matrix that was approved by the policy committee, what are the care goals that should be achieved on this? The second one is provide transparency of data sharing to the patient. That's different than providing patients with a copy of their data.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. I thought that that … so he's saying that they have no measures addressing that at all.

Deven McGraw - Center for Democracy & Technology – Director
There's actually, not only is there no measure, but there's no objective.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a good comment.

Deven McGraw - Center for Democracy & Technology – Director
In stage one. Now what you do have, of course, is a requirement to provide a notice of privacy practices under HIPAA. I think a lot of people are less than satisfied with that on both sides of the fence and find it not to be terribly useful, but that's what we have as of today.

Sarah Wattenberg – ONCHIT – Public Health Advisor
Deven, this is Sarah. What did the committee recommend for this category?

Deven McGraw - Center for Democracy & Technology – Director
We've got some notes here. I think we've got some things to say. What I had said was that, based on the comments, this is not our first bite at this apple, that I would put together some straw person, more specific recommendations so people would have a chance to review them before our next call, and we'd finalize them. But they were more in the area of finding some mechanism, whether it's through the regional extension centers or otherwise, to provide better education to providers and hospitals about how to do an appropriate risk assessment.

Sarah Wattenberg – ONCHIT – Public Health Advisor
No. I meant from, didn't the first policy committee provide recommendations for meaningful use?

Deven McGraw - Center for Democracy & Technology – Director
I still don't understand the question you're asking.

Sarah Wattenberg – ONCHIT – Public Health Advisor
I'm sorry. I thought that there were measures that were initially made by the policy group in August or whenever that was on specific meaningful use measures, and that there was one there for privacy. I just don't remember what it was, but I could be completely wrong.

Deven McGraw - Center for Democracy & Technology – Director
I'm getting it out, the matrix.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. In the NPRM on one of the tables of the meaningful use measures, that there's the capability to exchange key clinical information, and it's for both the eligible providers in the hospitals, and the description is store, send, and receive key clinical information on information transmitted to the providers and patient authorized entities. I'm wondering if that isn't somewhat of a hook for looking at support for privacy.

Deven McGraw - Center for Democracy & Technology – Director
What are you looking at again?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It's one of the tables in the CMS NPRM, and I can send this to you. I've got it taken out of the actual document, but it does talk about demonstrating the ability to store, send, and receive key clinical information, and it says, transmitting to providers and patient authorized entities. That, to a certain extent, seems to call for the ability to use patient authorizations to actually decide how information would be transmitted.

Deven McGraw - Center for Democracy & Technology – Director
Yes. But, Kathleen, that gets to the consent question that has a lot bigger ramifications. I know we're not going there yet. It's definitely on the agenda, but that's not necessarily a hook that we need to use, and it raises a lot of issues that we have not yet fully mined.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes. I don't think it's consent. I was thinking that it was the HIPAA authorization forms, and it's in the list of meaningful use measures, so that's why I'm bringing it up.
Deven McGraw - Center for Democracy & Technology – Director
Right, but I think you're cherry picking something out that has to do with – that's in another area.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I was just….

Deven McGraw - Center for Democracy & Technology – Director
I'm not sure we need it.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I was just looking for something. There was a question about was there anything in the meaningful use measures that related to privacy, and I was wanting to highlight that particular one. I don't feel like I'm particularly cherry picking.

Deven McGraw - Center for Democracy & Technology – Director
Okay. Yes. It's from another. I think Sarah's question was related to the privacy and security category of the meaningful use matrix, and it sounds like what you're quoting from is in another category … care goal.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes, it is. It's a different…. Yes, this is out of the rule, and Sarah was talking about what was in the matrix where, like, in 2015, there's segmentation, and there were some other ones for earlier periods.

Sarah Wattenberg – ONCHIT – Public Health Advisor
I see. There was nothing for the first year?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I think the first year was just HIPAA privacy.

Deven McGraw - Center for Democracy & Technology – Director
Yes. That's right. Kathleen is exactly right. And the risk assessment, so as we discussed earlier, the compliance with the privacy and security rule piece is full compliance with the rules was the piece that did not get picked up by CMS in the rule, but they did pick up the one measure for 2011 that was adopted by the policy committee, which was conducting or updating the security risk assessment.

Dave Wanser – NDIIC – Executive Director
This is Dave Wanser. Coming back to that issue, though, I think Kathleen's point is well taken that one of the ways of providing transparency of data sharing to the patient is through the use of a consent and

authorization process, and that's something that one can attest to. It's not the only way, but it certainly is a starting point for stage one. That's one of the ways that you can get at that issue.

Deven McGraw - Center for Democracy & Technology – Director
Can you explain more of what you mean by that?

Dave Wanser – NDIIC – Executive Director
Well, I think the concern that the care goal is speaking to is that patients' information should not be disclosed without their knowledge and consent.

Deven McGraw - Center for Democracy & Technology – Director
It's actually not, Dave. Is Paul Tang still on the line?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
I am.

Deven McGraw - Center for Democracy & Technology – Director
This is the question that we're talking about is the care goal that was identified in the meaningful use matrix in the privacy and security area specifically of providing transparency of data sharing to the patient, which was an established care goal, but for which we did not, you know, the only objectives that were established were compliance with the rules of HIPAA and the fair data sharing practices that are in the nationwide framework that we discussed earlier in the call with measures being limited to full compliance of the HIPAA privacy and security rules, and then conducting or updating a security risk assessment. I don't think that we intended that data transparency provision to mean consent per se because I think we recognize that that was a bigger issue that would need further discussion to resolve, but I don't want to speak out of turn if you think that that's not accurate.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
No, I think you're right. I think you're right, Deven. That was, in a sense, just a little bit like what we now call principles. So we wanted patients to understand how their data was being used and disclosed. In a sense, that comes back. That then translates into the principals that this group talked about in terms of the old framework or the previous framework, and goes into right now HIPAA privacy and security. And another thing for this group to think about is EHRs in the sense that in addition to what we've done with EHRs for the provider facing EHRs, we have that whole category of engaged patients and families. And what's going on there is we're giving access to and use of their data with the electronic tools and applications. So that automatically said there's a notion of a PHR going on, so that would imply that the privacy and security workgroup, this group, may have something to say about use and protection of information, as it resides and is disclosed through PHRs. I know that's a big can of worms, but in a sense that's something we already opened up with meaningful use for a good reason.

Deven McGraw - Center for Democracy & Technology – Director
Here's the thing about consent. We are absolutely going to take this issue on, absolutely, and it has a lot of very complicated components to it from what's capable with respect to from the vendor standpoint to what policy do we have in place today, and what we ought to be pursuing in the future. I promise you that we will do that, and the only reason why we're not starting with that is because there's some architecture of NHIN issues that are currently being discussed and upon which recommendations are being formulated by the NHIN workgroup, and we decided that we would hold off on beginning those conversations until we had a little bit more direction on what this network is going to look like. We will get there, but it's not – it doesn't do justice to the issue at all, I think, to attempt to shoehorn it into this space when we haven't necessarily had a conversation about it. And so, while I'm trying to think of what, if anything, I think we should think about what to do about this data sharing transparency issue, which is another important issue in privacy, and include when an individual has the right to consent and when they don't. I think, to try to take it on in a bigger way as part of this discussion in order to inform comments on meaningful use, we would never get it done in time to comment on this rule. It's just that….

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. I'm wondering though. It sounds as if the architecture of the NHIN is sort of setting the groundwork and the parameters for what this committee can discuss? Is that what I'm hearing?

Deven McGraw - Center for Democracy & Technology – Director
No, not necessarily, but it helps to shape. You know, a consent discussion is just much better informed if we know consent to what, like, what are we talking about? On the one hand, it's as broad as data sharing in any capacity. On the other hand, certainly the way that it's been shaping up, it was nationally, over the past couple of years, it's been enhanced with respect to network participation. And so, we were told that the NHIN workgroup would have some concrete things to say on this early in this year, and it seemed to make sense not to sort of necessarily begin those discussions until we had further information from them. Now I need to do a double-check on where they're headed because I'm not sure they're as far as we thought they were going to get. And I don't want to put this conversation off for much longer because it's going to take us some time.

Paul Egerman – eScription – CEO
This is Paul Egerman. I agree with what you just said, Deven. I think we really do need to know a lot about where NHIN is going, as we define privacy policy because otherwise it's the cart before the horse. But I'm also looking at the time clock. I know, in a couple minutes, we have to start the public comment section. Most of this discussion or the vast majority of the discussion has been on the NPRM, on the meaningful use side, and I'm wondering if … we've done very little discussion of the IFR piece. There's probably not enough time to broach that. Now whether or not we need to mark that for some additional discussion for a future meeting.

Deven McGraw - Center for Democracy & Technology – Director
No, absolutely, Paul. I totally agree with you. In fact, I invite folks. I actually started to hear Kathleen raise some concerns about something that she thought was missing. If other folks in the interim between now and our next call, which is in a couple of weeks, have things that they want to put on the table, send them to me early, please, because it'll help Rachel and I to structure the agenda so that we make sure that we get all of these points discussed. Again, it's always going to be a challenge with the number of people that we have in the group to moving this forward.

Paul Egerman – eScription – CEO
Yes, and my comment is also that that certification piece is a powerful, public policy tool that we have, and so the question is, is it being used correctly for this privacy and security piece, which we all agree is critically important. So that's also just an important issue to put some attention to.

M
Was Kathleen's comment about the access?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

M
Okay. Yes, that needs to. Yes.

Deven McGraw - Center for Democracy & Technology – Director
Kathleen, send me something since we're talking about your point that you didn't get to raise.

Rachel Block – New York eHealth Collaborative – Executive Director
Deven, this is Rachel. I've been listening carefully, and maybe somebody already made this comment or conclusion, but I wonder in terms of just dealing with the somewhat narrower question of the transparency if part of what we're doing is trying to crosswalk the certification criteria to the meaningful use. Since the certification criteria at least do address the auditing of disclosures, I wonder if there ought not to be

perhaps a recommendation from our group, if there was concensus, on a meaningful use measure relative to that certification criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I was just going to say. That would be, you know, we've been pointing out how the provide transparency has no objective or measures, and that's really where the hook is because accounting for disclosures is not even mentioned in the NPRM. It's just mentioned in the IRF, and this is really where it relates.

John Blair – Hudson Valley HIE – President & CEO
I don't want to keep harping on it, but that gets back into the thing that I was talking about before with risk assessment. If you start to include those kinds of things as minimum requirements for everyone, doesn't that get at that?

Rachel Block – New York eHealth Collaborative – Executive Director
Yes, but then we just have to go through the list, John, that we started doing of what we think key elements are. And I'm just not sure. It's one thing to have a security risk assessment and act on it, whatever that means. But I'm not sure if I would assume that that security risk assessment would address a patient's access to the audit log for disclosure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's right, and if you looked at the NPRM now, at page 64, you see that it has these two care goals, and then it only has one objective that it says addresses both of these care goals, but I would argue that protecting electronic health information through the implementation of appropriate technical capabilities does not necessarily include the accounting for disclosures.

Deven McGraw - Center for Democracy & Technology – Director
No, and that's also got some different timeframes for implementation that we'll have to think about in terms of crafting something.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, so what I'm suggesting is that we consider recommending that we add accounting for disclosures as an objective.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
But why would you? That's a duplication of the extension to HIPAA that ARRA applied. ARRA added to HIPAA to say no longer is TPO exempted from the disclosure, the accounting for disclosures. In a sense it's already done. Perhaps the language can be strengthened to say it's not just the HIPAA security piece we're interested in. It's also the HIPAA privacy rule, which has been modified by ARRA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and looking at what's in the NPRM, it doesn't mention HIPAA at all. It just says, protect electronic health information, created and maintained through the implementation of appropriate, technical capabilities. And accounting for disclosures is more than just technical capabilities.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Right. I think, if I remember correctly, the preamble piece, it talked about one of the reasons they sort of took HIPAA out is because it already exists, and people are expected to be compliant with it. That's a little bit of what I'm saying, but perhaps you're right. Maybe a suggestion is to tie HIPAA as part of meaningful use, and that just means it goes back to Deven's whole point. You need to be in compliance with HIPAA, both privacy and security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You just need a cross-reference.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Yes, it's almost a cross-reference rather than adding another, but duplicative, requirement.

Deven McGraw - Center for Democracy & Technology – Director
Right. We certainly wouldn't want to duplicate it. I'm going to have to – we're eating into our public comment period, and so I want to – Rachel and I will definitely talk about this a bit more and try to tee up some things that are a bit more specific for your consideration for the next call, and we'll also spend some more time talking about those security standards that are in the certification criteria, so definitely send in any comments really that you weren't able to sort of squeeze into this limited amount of time that we have on the call today.

W
Deven, when is the next call?

Judy Sparrow – Office of the National Coordinator – Executive Director
January 22nd, 10:00 to noon.

W
Thank you.

Deven McGraw - Center for Democracy & Technology – Director
Let's bring the public in.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes. Alison, can you do that, open up the lines? Then, Deven, if you have any final remarks you want to make while she opens up the public lines.

Deven McGraw - Center for Democracy & Technology – Director
Sure. Thanks to everyone for your patience. Again, these are – you know, I think it's hard sometimes to separate out some of these bigger issues that we know we need to resolve from maybe some others that we can tackle in this particular time period. But again, we'll just continue to do the best that we can, and I can't emphasize enough that we are not – that this issue of consent that is certainly on a lot of people's minds, front and center. We will deal with it, and we'll deal with it in a very comprehensive way.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. Operator, are there any public on the line for comment?

Operator
No, there are no public comments as of yet.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay.

Deven McGraw - Center for Democracy & Technology – Director
Give folks a couple more minutes.

Judy Sparrow – Office of the National Coordinator – Executive Director
All right.

Rachel Block – New York eHealth Collaborative – Executive Director
Deven, just in terms of our work plan and just the prioritization of timing, I think it probably goes without saying, but I'll say it while we're waiting is that some sort of a summary of potential issues or clarifications on the two rules would be the most important thing for us to try to tackle at our next discussion.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Rachel Block – New York eHealth Collaborative – Executive Director
And so, if members of the committee have either specific suggestions about some of the things that they commented on during the course of the call or any other issues, to get those to us before the next meeting would be the most timely way to insure they could be addressed.

Deven McGraw - Center for Democracy & Technology – Director
Yes. And as soon as possible actually because we'll have to start pulling an agenda together.

Rachel Block – New York eHealth Collaborative – Executive Director
Yes, because it's just barely two weeks.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Just to reinforce what Deven said about the timeline, the HIT Policy Committee is expected to … its deliberation on the comments on the NPRM by its next February meeting, which is—

Judy Sparrow – Office of the National Coordinator – Executive Director
February 17th.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
February 17th, and then will be submitting to ONC its comments by March 1st, so that's to keep with CMS's timeline. So the digested information from this workgroup needs to reach the MU or the meaningful use workgroup in time for it to make its presentation to the full committee by the February 17th date, so there's not a whole lot of time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anybody on the line, operator?

Operator
No, there's no one in line waiting.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you.

Deven McGraw - Center for Democracy & Technology – Director
All right.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thanks, everyone.

W
Thank you.

M
Thank you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you. Bye-bye.

Public Comments

1. Speaking of technology, forward looking idea: we know schools have their own frequency assigned to them, by the same token healthcare providers deserve to have one universal frequency for communication between the different providers (pharmacy, labs, hospitals, medical imaging services, etc), emergency vehicles and attending physician, telemedicine for disadvantaged communities. The new frequency can only be realized through the cooperation and vision of HHS secretary and FCC director; We are now in an era where the time, condition and other factors are right.